### ,/429

# RAPPORT D'EXAMEN PRELIMINAIRE INTÉRNATIONALC 2004

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire POUF				POUR SUITE A D	ONNER voir la notificati préliminaire int	on de transmission du rapport d'examen ernational (formulaire PCT/IPEA/416)		
Demande internationale No. PCT/IB 03/02425				Date du dépôt internation 10.06.2003	onal (jour/mois/année)	Date de priorité (jour/mols/année) 12.06.2002		
	sification		mationale des brevets (CIE	3) ou à la fois classification	n nationale et CIB			
Déposant NAGRACARD SA et al.								
1.	<ol> <li>Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.</li> </ol>							
2./	2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.							
/	II est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).							
	Ces annexes comprennent feuilles.							
Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :						es aux points suivants :		
	ı	☒	Base de l'opinion					
	11		Priorité					
	III   Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle							
	IV		Absence d'unité de l'in	vention				
	V Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration							
	VI		Certains documents ci	ités				
	VII		Irrégularités dans la de	emande internationale				
	VIII		Observations relatives	à la demande internat	ionale			
Date de présentation de la demande d'examen préliminaire internationale			en préliminaire	Date d'achèvement du p	orésent rapport			
20.12.2003					07.06.2004			
		interr	ostale de l'adminstration cl ational		Fonctionnaire autorisé	Andrew Constitution of the		
Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl				as	Holper, G			
Fax: +31 70 340 - 3016					N° de téléphone +31 70	340-2304		

#### RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n°

PCT/IB 03/02425

<ol> <li>Base du rappoi</li> </ol>	I.	B	ase	du	rap	ро	r
------------------------------------	----	---	-----	----	-----	----	---

1. En ce qui concerne les **éléments** de la demande internationale (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)):

	Des	cription, rages							
	1-13	3	telles qu'initialement déposées						
	Rev	Revendications, No.							
	1-16	6	telles qu'initialement déposées						
	Des	sins, Feuilles							
	1/2-	2/2	telles qu'initialement déposées						
2.	ou l	n ce qui concerne la <b>langue</b> , tous les éléments indiqués ci-dessus étaient à la disposition de l'administration u lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication ontraire donnée sous ce point.							
	Ces	éléments étaient à l	a disposition de l'administration ou lui ont été remis dans la langue suivante:	,qui est:					
		la langue d'une trade	uction remise aux fins de la recherche internationale (selon la règle 23.1(b)).						
		la langue de publica	tion de la demande internationale (selon la règle 48.3(b)).						
		la langue de la tradu 55.3).	uction remise aux fins de l'examen préliminaire internationale (selon la règle 55	.2 ou					
3.	inte	ce qui concerne les <b>s</b> rnationale (le cas éch uences :	séquences de nucléotides ou d'acide aminésdivulguées dans la demande néant), l'examen préliminaire internationale a été effectué sur la base du listage	des					
		contenu dans la den	nande internationale, sous forme écrite.						
		déposé avec la dem	nande internationale, sous forme déchiffrable par ordinateur.						
		remis ultérieuremen	t à l'administration, sous forme écrite.						
	remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.								
		La déclaration, selor de la divulgation fait	n laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas e dans la demande telle que déposée, a été fournie.	au-delà					
		La déclaration, selor à celles du listages d	n laquelle les informations enregistrées sous déchiffrable par ordinateur sont id des séquences Présenté par écrit, a été fournie.	entiques					
4.	Les	modifications ont en	traîné l'annulation :						
		de la description,	pages:						
		des revendications,	nos:						
		des dessins,	feuilles:						

#### RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n°

PCT/IB 03/02425

5. Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)):

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

- 6. Observations complémentaires, le cas échéant :
- V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- 1. Déclaration

Nouveauté Oui: Revendications 1-16

Non: Revendications

Activité inventive Oui: Revendications 1-16

Non: Revendications

Possibilité d'application industrielle Oui: Revendications 1-16

Non: Revendications

2. Citations et explications

voir feuille séparée

#### RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

#### Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant:

D1: WO 97/38530 (DIGCO)

La présente demande concerne un procédé d'échange sécurisé d'informations localement connectés entre eux ainsi qu'un récepteur pour la mise en oeuvre du dit procédé.

L'état de la technique le plus proche est illustré par D1 qui divulgue un procédé d'échange sécurisé d'informations entre un récepteur et un module de sécurité, les deux dispositifs étant localement connectés. Le récepteur comporte une clé publique tandis que le module de sécurité comporte une clé privée correspondante. Le procédé sert à échanger une clé de session aléatoire chiffrée par la clé publique.

Problème dans l'état de la technique: la clé de session peut être imposée par un intrus qui utiliserait ainsi une lacune de sécurité du procédé.

Selon la revendication 1 ce problème est résolu par les étapes consistant à générer un nombre aléatoire différent dans chaque dispositif, chiffrer ce nombre par la première respectivement la seconde clé de la paire de clés, transmettre le nombre chiffré à l'autre dispositif, déchiffrer les nombres chiffrés dans chaque dispositif et combiner lesdits nombres aléatoires pour générer une clé de session utilisée pour l'échange de données entre les deux dispositifs.

Un procédé basé sur le chiffrage de deux nombres aléatoires chiffrés par deux clés différentes de la même paire de clés n'est pas connu ni suggéré par l'état de la technique.

La revendication 1 remplit donc les critères de nouveauté et d'activité inventive de l'article 33(2) et (3) PCT.

Le récepteur selon la revendication 15 est arrangé pour la mise en oeuvre du procédé selon la revendication 1 et remplit donc aussi les critères de nouveauté et d'activité

BEST AVAILABLE COPY

## RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

inventive.

Les caractéristiques supplémentaires des revendications dépendantes 2-14 et 16 définissent des détails de réalisation de sorte que ces revendications sont aussi nouvelles et inventives.

Les procédés et récepteurs revendiqués présentent la possibilité d'activité industrielle.

BEST AVAILABLE COPY